

10/079,405
07/13/06

Reference 2

JP 2001-77857 A
[0003]

As a method of allowing the firewall 103 to realize such a security function, there is a method such as packet filtering. This packet filtering is performed as follows, for example. That is to say, as to a packet sent from the server 104 or the client 101, the firewall 103 determines whether to allow the packet to pass through, based on the IP address, the port number, etc, of the packet, the port number indicating the type of higher-ranked applications. A packet that is allowed to pass through is transferred to a counterpart as it is.

THIS PAGE BLANK COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-077857

(43)Date of publication of application : 23.03.2001

(51)Int.Cl.

H04L 12/56

G06F 13/00

H04L 12/28

H04L 12/66

(21)Application number : 11-253871

(71)Applicant : PFU LTD

(22)Date of filing : 08.09.1999

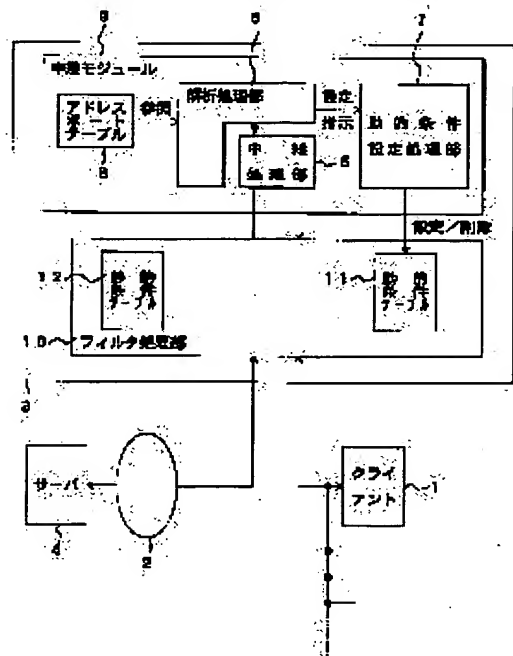
(72)Inventor : YAMAMOTO MASAO

(54) FILTERING PROCESSING DEVICE, NETWORK PROVIDED WITH IT AND ITS STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance the security of clients in a filtering processing device.

SOLUTION: The filtering processing device 3 is provided between a client 1 and a sever 4 to filter data sent/received between them. The filtering processing device 3 is provided with an analysis processing section 6 and a dynamic condition setting processing section 7. The analysis processing section 6 analyzes data sent from the client 1 to the server 4. The dynamic condition setting processing section 7 sets a filtering conditions as to data sent from the server 4 to the client 1 on the basis of the analysis result by the analysis processing section 6.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (COPY)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-77857

(P2001-77857A)

(43) 公開日 平成13年3月23日 (2001.3.23)

(51) Int.Cl. ⁷	識別記号	F I	データ* (参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 A 5 B 0 8 9
G 0 6 F 13/00	3 5 1	C 0 6 F 13/00	3 5 1 Z 5 K 0 3 0
H 0 4 L 12/28		H 0 4 L 11/00	3 1 0 D 5 K 0 3 3
12/66		11/20	B

審査請求 未請求 請求項の数12 O L (全 11 頁)

(21) 出願番号 特願平11-253871

(22) 出願日 平成11年9月8日 (1999.9.8)

(71) 出願人 000136136

株式会社ビーエフユー

石川県河北郡宇ノ気町宇字野気ヌ98番地の
2

(72) 発明者 山本 昌夫

石川県河北郡宇ノ気町宇字野気ヌ98番地の
2 株式会社ビーエフユー内

(74) 代理人 100074848

弁理士 森田 寛 (外1名)

最終頁に続く

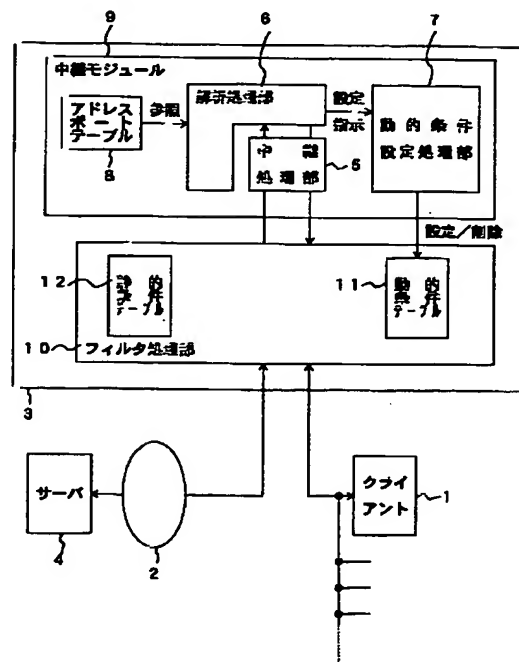
(54) 【発明の名称】 フィルタリング処理装置及びこれを備えるネットワーク及びその記憶媒体

(57) 【要約】

【課題】 本発明は、フィルタリング処理装置に関し、クライアントのセキュリティを向上することを目的とする。

【解決手段】 フィルタリング処理装置3はクライアント1とサーバ4との間に設けられ、これらの間において送受信されるデータのフィルタリングを行う。フィルタリング処理装置3は解析処理部6と動的条件設定処理部7とを備える。解析処理部6はクライアント1からサーバ4に対して送信されるデータを解析する。動的条件設定処理部7は、解析処理部6における解析結果に基づいて、サーバ4からクライアント1に対して送信されるデータについてのフィルタリングの条件を設定する。

フィルタリング処理装置説明図



【特許請求の範囲】

【請求項1】 クライアントとサーバとの間に設けられ、これらの間において送受信されるデータのフィルタリングを行うフィルタリング処理装置であって、前記クライアントから前記サーバに対して送信されるデータを解析する解析処理部と、前記解析処理部における解析結果に基づいて、前記サーバから前記クライアントに対して送信されるデータについてのフィルタリングの条件を設定する動的条件設定処理部とを備えることを特徴とするフィルタリング処理装置。

【請求項2】 前記クライアントとサーバとの間において送受信されるデータはパケットからなることを特徴とする請求項1に記載のフィルタリング処理装置。

【請求項3】 当該フィルタリング処理装置が、更に、前記動的条件設定処理部により設定された条件に従って、当該フィルタリング処理装置を通過しようとするデータについてのフィルタリングを行うフィルタ処理部を備えることを特徴とする請求項1に記載のフィルタリング処理装置。

【請求項4】 前記解析処理部の解析するデータは、前記クライアントからの前記サーバに対する第1のコネクションを介して、前記クライアントから送信されるデータであり、前記動的条件設定処理部の設定する条件は、前記第1のコネクションに対応する前記サーバからの前記クライアントに対する第2のコネクションを介して、前記サーバから送信されるデータについてのフィルタリングの条件であることを特徴とする請求項1に記載のフィルタリング処理装置。

【請求項5】 前記解析処理部の解析するデータは、前記サーバ及びクライアントの間における前記第2のコネクションについての制御情報を含むことを特徴とする請求項4に記載のフィルタリング処理装置。

【請求項6】 前記第2のコネクションについての制御情報は、前記第2のコネクションを開設するための制御情報であり、前記第2のコネクションを開設するための制御情報に基づいて、前記動的条件設定処理部が前記フィルタリングの条件を設定することを特徴とする請求項5に記載のフィルタリング処理装置。

【請求項7】 前記第2のコネクションについての制御情報は、前記第2のコネクションを閉塞するための制御情報であり、前記第2のコネクションを閉塞するための制御情報に基づいて、前記動的条件設定処理部が前記フィルタリングの条件を削除することを特徴とする請求項5に記載のフィルタリング処理装置。

【請求項8】 前記クライアントからの前記サーバに対する第1のコネクションが存在する場合に、

前記解析処理部が、前記クライアントから送信されるデータを解析し、

前記動的条件設定処理部が、前記解析結果に基づいて、前記第1のコネクションに対応する前記サーバからの前記クライアントに対する第2のコネクションにおいて前記サーバから送信されるデータについてのフィルタリングの条件を設定することを特徴とする請求項1に記載のフィルタリング処理装置。

【請求項9】 前記クライアントからの前記サーバに対する第2のコネクションが存在する場合に、前記解析処理部が、前記クライアントから送信されるデータを解析し、

前記動的条件設定処理部が、前記解析結果に基づいて、前記第2のコネクションにおけるフィルタリングの条件を削除することを特徴とする請求項8に記載のフィルタリング処理装置。

【請求項10】 前記解析処理部が、第2のコネクションにおけるフィルタリング以外のフィルタリングについての条件を備えることを特徴とする請求項1に記載のフィルタリング処理装置。

【請求項11】 クライアントと、サーバと、

前記クライアントとサーバとの間に設けられ、これらの間において送受信されるデータのフィルタリングを行うフィルタリング処理装置とを備え、

前記フィルタリング処理装置が、前記クライアントから前記サーバに対して送信されるデータを解析する解析処理部と、

前記解析処理部における解析結果に基づいて、前記サーバから前記クライアントに対して送信されるデータについてのフィルタリングの条件を設定する動的条件設定処理部と、

前記動的条件設定処理部により設定された条件に従って、当該フィルタリング処理装置を通過しようとするデータについてのフィルタリングを行うフィルタ処理部を備えることを特徴とするネットワーク。

【請求項12】 クライアントとサーバとの間において送受信されるデータのフィルタリングを行うプログラムを格納したコンピュータ読取可能な記憶媒体において、当該プログラムは、

前記クライアントから前記サーバに対して送信されるデータを解析する第1のプログラムコードと、

前記解析結果に基づいて、前記サーバから前記クライアントに対して送信されるデータについてのフィルタリングの条件を設定する第2のプログラムコードとを有することを特徴とするコンピュータ読取可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、フィルタリング処理装置及びこれを備えるネットワーク及びその記憶媒体

に関し、特に、クライアントのセキュリティを向上したフィルタリング処理装置及びこれを備えるネットワーク及びその記憶媒体に関する。

【0002】

【従来の技術】インターネットにおいては、クライアント（WWWブラウザ）に対して、種々のサーバが接続してくる。そこで、セキュリティの確保のために、図7（A）に示すように、インターネット102とクライアント101との間にファイアウォール103が設けられる。クライアント101又はサーバ104から送出されたパケットは、ファイアウォール103を通過することが認められれば、これを越えて通信の相手方に到達することができる。

【0003】ファイアウォール103がこのようなセキュリティ機能を実現する方法には、例えばパケットフィルタリング等の方法がある。このパケットフィルタリングは、例えば、以下のように行われる。即ち、サーバ104又はクライアント101から送られたパケットについて、ファイアウォール103が、パケットのIPアドレスや上位アプリケーションの種類を示すポート番号等に基づいて、当該パケットを通過させるか否かを決定する。通過させると決定されたパケットは、そのまま相手方に転送される。

【0004】

【発明が解決しようとする課題】大量のデータ転送を頻繁に行うようなネットワークでは、通信経済の観点から、通常、クライアント101とサーバ104との間の通信は、以下のように行われる。即ち、クライアント101からサーバ104への接続（以下、第1のコネクションと言う）を確立し、この第1のコネクションによりクライアント101からサーバ104へ要求を通知するための制御用の通信を行う。次に、第1のコネクションとは別に、サーバ104からクライアント101への接続（以下、第2のコネクションと言う）を確立し、この第2のコネクションによりデータ送信用の通信を行う。第2のコネクションにおいては、一般に、既に接続済の通信路を使用した通信の待ち合わせ又は受信ポートの指定が可能である。

【0005】そこで、ファイアウォール103を採用するネットワークにおいて、上記第2のコネクションを許す場合、ファイアウォール103に、当該第2のコネクションにおけるパケットについてのパケットフィルタリング（通過）の条件を、予め設定しておく必要がある。

【0006】このような第2のコネクションについてのパケットフィルタリングの一例として、例えばFTP（ファイルトランスファプロトコル）の場合について説明する。FTPにおいては、データ転送時にサーバ104の固定ポート（ポート番号20）からクライアント101のANYポートに接続する（コネクションを確立する）。ここで、ANYポートは、サーバ104がクラ

イアント101からの通知に基づいて当該通信毎に割り当てるポートであり、そのポート番号は予め1024～65535の範囲とされる。従って、第2のコネクションについてのパケットフィルタリングの条件テーブル111は、図7（B）に示すように、送信先のポート番号が1024～65535であるパケットについて通過させる設定とされる。即ち、ファイアウォール103は、サーバIPアドレスSのポート番号20からのクライアントIPアドレスCへのパケットについては、送信先のポート番号が1024～65535の範囲であれば、通過させることになる。

【0007】このため、第2のコネクションにおいては、クライアント101から見ると、サーバIPアドレスSのポート番号20からのパケットであれば、ポート番号が1024～65535と言う広範囲のものがファイアウォール103を通過する。従って、極めて広範囲のパケットについて、ファイアウォール103が存在しないように見えることになる。即ち、ファイアウォール103の内側に保護されているはずのクライアント101が、極めて広範囲のパケットについて無防備な状態に置かれていることになる。

【0008】本発明は、クライアントのセキュリティを向上したフィルタリング処理装置を提供することを目的とする。

【0009】また、本発明は、クライアントのセキュリティを向上したネットワークを提供することを目的とする。

【0010】また、本発明は、クライアントのセキュリティを向上したフィルタリング処理装置を実現するプログラムを記憶する記憶媒体を提供することを目的とする。

【0011】

【課題を解決するための手段】図1は本発明の原理構成図であり、本発明によるフィルタリング処理装置3を示す。フィルタリング処理装置3はクライアント1とサーバ4との間に設けられ、これらの間において送受信されるデータのフィルタリングを行う。フィルタリング処理装置3は解析処理部6と動的条件設定処理部7とを備える。解析処理部6はクライアント1からサーバ4に対して送信されるデータを解析する。動的条件設定処理部7は、解析処理部6における解析結果に基づいて、サーバ4からクライアント1に対して送信されるデータについてのフィルタリングの条件を設定する。

【0012】本発明のフィルタリング処理装置3によれば、クライアント1からサーバ4に対して送信されるデータの解析結果に基づいて、サーバ4からクライアント1に対して送信されるデータについてのフィルタリングの条件を動的に設定することができる。従って、当該条件を満たすデータのみがフィルタリング処理装置3を通過するように設定することができる。例えば、前述のよ

うに第2のコネクションを許す場合、クライアント1からサーバ4へのデータから、クライアント1におけるデータの送受信の条件を検出する。これにより、第2のコネクションにおいてサーバ4からクライアント1へのデータがどのような条件で送信されるかを予め知り、これに基づいて、サーバ4からクライアント1へのデータの内で当該送信の条件に合致するデータのみが、第2のコネクションにおいてフィルタリング処理装置3を通過するように設定することができる。従って、第2のコネクションにおいて、クライアント1から見て、同一のサーバ4からのデータであっても、フィルタリングの条件を満たさないデータはフィルタリング処理装置3を通過することができない。これにより、クライアント1をフィルタリング処理装置3の内側に保護することができ、そのセキュリティを向上することができる。

【0013】

【発明の実施の形態】図2はフィルタリング処理装置説明図であり、本発明のフィルタリング処理装置3及びこれを備えるネットワークの構成を示す。

【0014】図2において、フィルタリング処理装置3は、例えばファイアウォール3からなる。ファイアウォール3は、クライアント1のセキュリティの確保のために、ネットワーク2とクライアント1との間に設けられ、フィルタリングを行う。従って、サーバ4から見た場合、クライアント1はファイアウォール3の内側にあり、これにより守られている。例えば、(複数の)クライアント1はファイアウォール3と共にイントラネットを構成する。ネットワーク2は、例えばインターネット2からなる。サーバ4はウェブ(Web)サーバやプロキシサーバ等からなる。従って、全体をネットワークとして見ると、クライアント1、サーバ4、ファイアウォール3とを備える。

【0015】クライアント1は、例えば、インターネット2を介して、サーバ4にアクセスする。この時、クライアント1は、ファイアウォール3にアクセスしてそのフィルタ処理部10を通過する必要がある。逆に、クライアント1に応答するサーバ4も、ファイアウォール3にアクセスしてそのフィルタ処理部10を通過する必要がある。従って、ファイアウォール3は、その内側のクライアント1(の属するイントラネット)と外側のインターネット2とを切り離す。フィルタ処理部10を通過すれば、クライアント1とサーバ4とはファイアウォール3を越えて相互にアクセスすることができる。

【0016】ファイアウォール3は、中央演算処理装置(CPU)、主メモリ、補助記憶等(いずれも図示せず)からなる。主メモリ上に、フィルタリング処理を行うプログラムが存在する。フィルタリング処理プログラムがCPU上で実行されることにより、以下に説明する各処理部5、6、7、10によるフィルタリング処理が行われる。なお、アドレスポートテーブル8、動的条件

テーブル11、静的条件テーブル12は磁気ディスク装置等の補助記憶に設けられる。

【0017】ファイアウォール3は、前述のように、クライアント1のセキュリティの実現のために、クライアント1とサーバ4との間に設けられ、これらの間において送受信されるデータのフィルタリング処理を行う。クライアント1とサーバ4との間において送受信されるデータはパケットからなる。従って、ファイアウォール3はパケットフィルタリングによりクライアント1のセキュリティを実現する。このために、ファイアウォール3は、中継モジュール9、フィルタ処理部10を備える。中継モジュール9は、フィルタ処理部10を制御し、また、そのための制御情報(フィルタリングの制御のための情報)を作成する。フィルタ処理部10は、中継モジュール9の制御に従って、クライアント1又はサーバ4から受信したパケットについてのフィルタリングを行う。中継モジュール9は、中継処理部5、解析処理部6、動的条件設定処理部7を備える。

【0018】フィルタ処理部10は、動的条件設定処理部7により設定された条件に従って、当該ファイアウォール3を通過しようとするデータについての実際のフィルタリング処理及び通信処理を行う。即ち、フィルタ処理部10は、クライアント1又はサーバ4から送信されてきたパケットの受信処理を行い、フィルタリングの制御のための情報(動的フィルタリング情報)を抽出するために、これを中継モジュール9に送る。また、フィルタ処理部10は、中継モジュール9からのパケットを受け取り、予め自己が備えるフィルタリングの制御のための情報(静的フィルタリング情報)と中継モジュール9から与えられたフィルタリングの制御のための情報(動的フィルタリング情報)とに従ってフィルタリングした後、通過させるべきパケットの当該クライアント1又はサーバ4への送信処理を行う。

【0019】このために、フィルタ処理部10は、図3(B)に示すように、動的条件テーブル11を備える。動的条件テーブル11は、中継モジュール9からのフィルタリングの制御のための情報(動的フィルタリング情報)を格納する。動的フィルタリング情報は、第2のコネクションにおけるフィルタリングについての条件を規定する情報である。動的フィルタリング情報は、後述するように、動的条件設定処理部7により設定され、削除される。

【0020】フィルタ処理部10は、動的条件テーブル11とは別に、第2のコネクションにおけるフィルタリング以外のフィルタリング(例えば、第1のコネクションにおけるフィルタリング)についての条件(静的フィルタリング情報)を備える。このために、フィルタ処理部10は、図3(A)に示すように、静的条件テーブル12を備える。静的条件テーブル12は、静的フィルタリング情報を格納する。静的フィルタリング情報は、第

1のコネクションにおけるフィルタリングについての条件を規定する情報である。

【0021】図3(A)に示す静的条件テーブル12は、例えばFTPの場合について示す。FTPにおいては、処理「通過」の対象として、送信元アドレスとしてクライアント1の「クライアントIPアドレスC」、そのポート(送信元ポート)番号として「1024~65535」、送信先アドレスとしてサーバ4の「サーバIPアドレスS」、そのポート(送信先ポート)番号として「21」が設定される。クライアント1の送信ポート番号が「1024~65535」のように広範囲であるが、ファイアウォール3の内側であるので、セキュリティ上の問題はない。サーバ4の受信ポート番号「21」は固定である。従って、第1のコネクションについてのパケットフィルタリング(静的フィルタリング)は、クライアントIPアドレスCのポート番号1024~65535からのサーバIPアドレスSのポート番号21へのパケットについては、通過させることになる。

【0022】また、このようなパケットに対する第1のコネクション上の応答パケットについても、通過させることになる。例えば、クライアント1からのパケットの送信ポートが1024であるとする、サーバIPアドレスSのポート番号21からのクライアントIPアドレスCのポート番号1024へのパケットについても、通過させることになる。これは、一旦確立された第1のコネクションに接続する特定のサーバ4及びクライアント1の間での通信であり、かつ、一旦静的フィルタリングを通過した送受信のポートの間での通信だからである。即ち、同一のクライアント1及びサーバ4の間の同一のポートでの通信だからである。

【0023】このために、フィルタ処理部10は、図3(A)に示す静的条件テーブル12において、処理「通過」の対象として、送信元アドレスとしてサーバ4の「サーバIPアドレスS」、そのポート(送信元ポート)番号として「21」、送信先アドレスとしてクライアント1の「クライアントIPアドレスC」、そのポート(送信先ポート)番号として「1024」を設定する。このフィルタリングの条件は、図3(A)に示す条件の裏返しの条件である。

【0024】中継モジュール9において、中継処理部5はデータの中継を行う。即ち、中継処理部5は、フィルタ処理部10からパケットを受け取り、動的フィルタリング情報を抽出するために、これを解析処理部6へ送る。また、中継処理部5は、解析処理部6からパケットを受け取り、フィルタリングのために、これをフィルタ処理部10に送る。

【0025】解析処理部6は、クライアント1からサーバ4に対して送信されるデータを解析する。具体的には、解析処理部6の解析するデータは、クライアント1からサーバ4に対して確立されたコネクション(第1の

コネクション)を介して、クライアント1から送信されるデータである。このデータは、第1のコネクションとは別に、サーバ4からクライアント1に対してその時点以後に確立される(又はその時点前に確立された)コネクション(第2のコネクション)についての情報を含む。第2のコネクションについての情報は、第2のコネクションを開設するための情報、又は、第2のコネクションを閉塞するための情報である。

【0026】この明細書において、第1及び第2のコネクションは、トランスポート層でのTCP(トランスミッションコントロールプロトコル)の接続である。第2のコネクションは、第1のコネクションが確立された後にそれが存在する状態で確立され、クライアント1からサーバ4へのコネクションである第1のコネクションとは逆に、サーバ4からクライアント1へのコネクションである。従って、第2のコネクションは、第1のコネクションの存在が前提であって、前提である当該第1のコネクションに対応する。

【0027】前述のように、パケットフィルタリングにおいては、パケットのIPアドレスや上位アプリケーションの種類を示すポート番号等に基づいて、当該パケットを通過させるか否かを決定する。従って、解析処理部6は、第2のコネクションを使用するネットワークアプリケーションのプロトコルデータを解析し、IPアドレスやポート番号等の接続に関する情報を、第2のコネクションについての情報として取得する。

【0028】例えば、FTPにおいては、第1のコネクションを介して、第2のコネクションについての情報が、所定のコマンドによりクライアント1からサーバ4に通知される。具体的には、クライアント1からのポート(PORT)コマンド及びこれに続くデータ受信コマンドにより、当該第1のコネクションを介しての通信の後、サーバ4からクライアント1への第2のコネクションが確立される。データ受信コマンドとしてはLIST、RETR又はSTOR等がある。また、当該ポートコマンドにより、第2のコネクションの利用時にクライアント1においてデータを受信するポートのアドレス及び当該ポートについての情報が、クライアント1からサーバ4に通知される。この情報は、(ASCII)文字列として通知され、例えば、ポートアドレス「192.168.1.1.4.1」と、IPアドレス「192.168.1.1」とポート番号「1025」とからなる(図3(B)参照)。

【0029】従って、解析処理部6は、第1のコネクション上のクライアント1からのパケットを解析し、ポートコマンドに続くデータ受信コマンドを検出すると、ポートコマンドにおける前記3個のデータを第2のコネクションについてのそれを開設させるための情報として抽出する。従って、第2のコネクションを用いた通信のフィルタリングにおいては、当該IPアドレスのクライアント1の当該ポート(及びアドレス)に対して当該サー

バ4から送信されるパケットのみを通過させれば良い。

【0030】また、クライアント1からのポートコマンド及びこれに続くデータ受信完了コマンドにより、当該第1のコネクションを介しての通信の後、第2のコネクションが閉塞される。従って、解析処理部6は、第1のコネクション上のクライアント1からのパケットを解析し、ポートコマンドに続くデータ受信完了コマンドを検出すると、前記と同様にポートコマンドにおける前記3個のデータを第2のコネクションについてのそれを閉塞させるための情報として抽出する。

【0031】なお、実際は、第1のコネクションに対して既に第2のコネクションが開設された状態で、更に、ポートコマンド及びこれに続くデータ受信コマンドが検出されると、当該既設の第2のコネクションは閉塞され、これとは別に新たな第2のコネクションが開設される。従って、既設の第2のコネクションについての動的フィルタリング条件は削除され、新たな第2のコネクションについての動的フィルタリング条件が設定される。

【0032】解析処理部6は、第2のコネクションにおけるフィルタリングについての条件（動的フィルタリング情報）を作成するために、アドレスポートテーブル8を備える。アドレスポートテーブル8は、アドレスポート情報を格納する。アドレスポート情報は、第2のコネクションが対応する第1のコネクションのサーバ4のサーバIPアドレスとそのデータ送信ポートとからなる。

【0033】例えば、FTPにおいては、サーバ4におけるデータの送信ポートは、第1のコネクションのサーバIPアドレス「192.168.1.1」と固定ポート20番とに固定されている。これらが、サーバ4についてのアドレスポート情報として、当該アドレスポートテーブル8に格納される。

【0034】従って、FTPにおいては、解析処理部6により、図3(B)に示すように、動的フィルタリング情報が作成される。即ち、前述の3個のデータの内、ポートアドレス「192.168.1.1.4.1」を用いてサーバ4のサーバIPアドレスを求め、また、当該ポートアドレスを用いてアドレスポートテーブル8を参照し、当該アドレスのサーバ4のデータ送信（送信元）ポート（ポート番号20）を求める。このポート番号20は、前述のように、固定である。また、3個のデータの内、IPアドレス「192.168.1.1」をクライアント1のクライアントIPアドレスとし、ポート番号「1025」をクライアント1のデータ受信（送信先）ポートとする。これにより、第2のコネクションにおいて、サーバ4から送信されるパケットは、送信先ポートが1025であるもののみがフィルタリングを通過できることになる。

【0035】動的条件設定処理部7は、解析処理部6における解析結果に基づいて、サーバ4からクライアント1に対して送信されるデータについてのフィルタリングの条件（動的フィルタリング情報）を設定する。具体的

には、動的条件設定処理部7の設定する条件は、第1のコネクションに対応するサーバ4からのクライアント1に対する第2のコネクションを介して、サーバ4から送信されるデータについての動的フィルタリングの条件である。従って、動的条件設定処理部7は、第2のコネクションを開設するための情報に基づいて動的フィルタリングの条件を設定し、又は、第2のコネクションを閉塞するための情報に基づいて動的フィルタリングの条件を削除する。

【0036】クライアント1からのサーバ4に対する第1のコネクションが存在する場合に、第2のコネクションについての動的フィルタリングの条件が設定される。具体的には、第2のコネクションの使用（又は設定）の直前に、その直前に行われた第1のコネクションを使用した通信を解析した結果に基づいて設定される。即ち、動的に設定される。このために、解析処理部6が、クライアント1から送信されるデータを解析し、動的条件設定処理部7が、この解析結果に基づいて、第1のコネクションに対応するサーバ4からのクライアント1に対する第2のコネクションにおいて、サーバ4から送信されるデータについてのフィルタリングの条件を動的に設定する。従って、第2のコネクションにおけるフィルタリングの条件を、必要な場合にのみ、その直前に動的に設定し、フィルタリングを行うことができる。

【0037】また、クライアント1からのサーバ4に対する第2のコネクションが存在する場合に、動的フィルタリングの条件が削除される。具体的には、第2のコネクションの使用（又は切断）の直後に、その直後に行われた第1のコネクションを使用した通信を解析した結果に基づいて、削除される。即ち、動的に削除される。このために、解析処理部6が、クライアント1から送信されるデータを解析し、動的条件設定処理部7が、解析結果に基づいて、第2のコネクションにおける動的フィルタリングの条件を削除する。従って、第2のコネクションにおけるフィルタリングの条件を、その直後に動的に削除することができる。

【0038】なお、実際は、第2のコネクションが対応する第1のコネクションが切断される場合、当該第2のコネクションも切断（閉塞）される。従って、この場合にも、その動的フィルタリングの条件が削除される。具体的には、クライアント1からサーバ4に対して第1のコネクションの切断が通知されたら、これを解析処理部6が検出して、動的条件設定処理部7により当該第2のコネクションが閉塞される。

【0039】例えば、前述のFTPにおいては、動的条件設定処理部7は、解析処理部6により図3(B)に示すように作成された動的フィルタリング情報を当該情報の設定指示と共に受け取り、当該情報をフィルタ処理部10の動的条件テーブル11に書き込む。これにより、フィルタ処理部10における動的フィルタリングの条件

が設定される。この結果、第2のコネクションにおいて、サーバ4から送信されるパケットは、送信先ポートが1025であるもののみがフィルタリングを通過できることになる。

【0040】図4は、ファイアウォール3が実行するフィルタリング処理フローを示す。

【0041】フィルタ処理部10が、パケットを受信したか否かを調べる（ステップS1）。受信していない場合、ステップS1を繰り返す。

【0042】受信した場合、フィルタ処理部10が、静的条件テーブル12及び動的条件テーブル11を用いて、静的フィルタリング処理及び動的フィルタリング処理を行う（ステップS2）。この時、フィルタ処理部10は、当該パケットが第1又は第2のコネクション上のものか及びクライアント1又はサーバ4からのものかを意識することではなく、また、静的フィルタリングか動的フィルタリングかを意識することはない。

【0043】フィルタ処理部10が、フィルタリング処理の結果、当該パケットが通過の条件を満足するか否かを調べる（ステップS3）。

【0044】満足する場合、フィルタ処理部10が、当該パケットを中継モジュール9に送る（ステップS4）。当該パケットは、中継モジュール9において、中継処理部5を介して、解析処理部6に送られる。

【0045】解析処理部6が、当該パケットを解析する（ステップS5）。

【0046】この解析の結果に基づいて、所定の処理が行われる（ステップS6）。これについては、図5を参照して後述する。

【0047】解析処理部6が、当該パケットをフィルタ処理部10に送る（ステップS7）。

【0048】フィルタ処理部10が、当該パケットを中継処理する（ステップS8）。即ち、当該パケットをその宛て先（送信先）に転送する。

【0049】ステップS3において通過の条件を満足しない場合、フィルタ処理部10が、当該パケットを廃棄する（ステップS9）。

【0050】図5は、図4のステップS6においてファイアウォール3が実行するフィルタリング条件設定処理フローを示す。

【0051】解析処理部6が、中継処理部5から受け取ったパケットについて解析する（ステップS11）。

【0052】解析処理部6が、当該解析結果に基づいて、第2のコネクションの開設についての情報が否かを調べる（ステップS12）。当該情報でない場合、ステップS15に進む。なお、このパケットは、フィルタ処理部10がクライアント1から受け取って中継処理部5に渡し、更に、中継処理部5が解析処理部6に渡したものである。

【0053】当該情報である場合、解析処理部6が、当

該解析結果に基づいて、第2のコネクションにおけるパケットフィルタリングの条件を作成し、動的条件設定処理部7に条件の設定を依頼する（ステップS13）。

【0054】依頼を受けた動的条件設定処理部7が当該条件をフィルタ処理部10に設定する（ステップS14）。この後、中継処理部5がパケットの中継処理を行う（図4のステップS7及びS8）。即ち、解析処理部6が、必要に応じてパケットのデータを書き替えた上で、当該パケットをフィルタ処理部10に返し、フィルタ処理部10が当該パケットをサーバ4に送信する。

【0055】ステップS12において第2のコネクションの開設についての情報でない場合、更に、解析処理部6が、第2のコネクションの閉塞についての情報が否かを調べる（ステップS15）。当該情報でない場合、図4のステップS7に進む。

【0056】当該情報である場合、解析処理部6が、当該解析結果に基づいて、第2のコネクションにおけるパケットフィルタリングの条件の削除を、動的条件設定処理部7に依頼し、依頼を受けた動的条件設定処理部7が、当該条件をフィルタ処理部10から削除する（ステップS16）。

【0057】図6は、クライアント1とサーバ4との間における通信について、ファイアウォール3が実行するフィルタリング処理説明図を示す。

【0058】クライアント1からファイアウォール3を介してサーバ4に対するコネクション（第1のコネクション）を張る（①）。

【0059】クライアント1が、第1のコネクション上でサーバ4に対する制御用のパケットを送信すると、ファイアウォール3が図3（A）に示す静的フィルタリング条件によりフィルタリングを行い（②のa）、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればサーバ4に転送する（②）。この時、当該パケットがクライアント1からのものであるため、解析処理部6が当該パケットを解析する。この結果、第2のコネクションを開設するための情報が抽出されないため、動的条件設定処理部7による動的フィルタリング条件の設定は行われない。

【0060】パケットを受信したサーバ4が、クライアント1に対する応答のパケットを送信すると、ファイアウォール3が図3（A）に示す静的フィルタリング条件の裏返しの条件によりフィルタリングを行い（③のa）、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればクライアント1に転送する（③）。

【0061】クライアント1がサーバ4に対するデータ転送要求（制御用）のパケットを送信すると、ファイアウォール3が図3（A）に示す静的フィルタリング条件によりフィルタリングを行い（④のa）、当該パケットを通過させるか否かを判断し、条件を満たすパケットで

あればサーバ4に転送する(④)。この時、当該パケットがクライアント1からのものであるため、解析処理部6が当該パケットを解析する。この結果、第2のコネクションを開通するための情報が抽出されるので、動的条件設定処理部7により、フィルタ処理部10の動的条件テーブル11への図3(B)に示す動的フィルタリング条件の設定が行われる。

【0062】パケットを受信したサーバ4が、第1のコネクションとは別に、当該サーバ4からファイアウォール3を介してクライアント1に対するコネクション(第2のコネクション)を張る(⑤)。

【0063】サーバ4が、クライアント1に対する転送データのパケットを送信すると、ファイアウォール3が図3(B)に示す動的フィルタリング条件によりフィルタリングを行い(⑥のb)、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればクライアント1に転送する(⑥)。

【0064】データを受信したクライアント1は、サーバ4に対するデータ受信完了通知(制御用)のパケットを送信すると、ファイアウォール3が図3(A)に示す静的フィルタリング条件によりフィルタリングを行い(⑥のa)、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればサーバ4に転送する(⑥)。この時、当該パケットがクライアント1からのものであるため、解析処理部6が当該パケットを解析する。この結果、第2のコネクションを閉塞するための情報が抽出されるので、動的条件設定処理部7により、フィルタ処理部10の動的条件テーブル11からの図3(B)に示す動的フィルタリング条件の削除が行われる。

【0065】サーバ4が、当該サーバ4からクライアント1に対するコネクション(第2のコネクション)を切断する(⑦)。

【0066】以上、本発明をその実施の態様により説明したが、本発明はその主旨の範囲において種々の変形が可能である。

【0067】例えば、動的フィルタリング条件の作成は、解析処理部6ではなく、動的条件設定処理部7又はフィルタ処理部10が行ってもよい。また、解析処理部6と動的条件設定処理部7とを一体に設けてもよい。

【0068】また、本発明は、FTPに限らず、例えばtelnet等の種々の通信プロトコルに適用すること

ができる。例えば、telnetにおいては、フィルタ処理部10における静的フィルタリングの後、そのまま中継処理を行うのではなく、当該パケットを中継モジュール9に送るようにすればよい。

【0069】

【発明の効果】以上説明したように、本発明によれば、フィルタリング処理装置において、第1のコネクションにおいてクライアントからサーバに対して送信されるデータの解析結果に基づいて、第2のコネクションにおいてサーバからクライアントに対して送信されるデータについてのフィルタリングの条件を動的に設定することにより、第2のコネクションにおいてサーバからクライアントへのデータがどのような条件で送信されるかを予め知ることができるので、当該送信の条件に合致するサーバからクライアントへのデータのみがフィルタリング処理装置を通過するように設定することができ、結果として、第2のコネクションにおいて通過条件を満たさないデータをフィルタリング処理により除去することができ、クライアントをフィルタリング処理装置の内側に保護してそのセキュリティを向上することができる。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】フィルタリング処理装置説明図である。

【図3】フィルタリング条件説明図である。

【図4】フィルタリング処理フローチャートである。

【図5】フィルタリング条件設定処理フローチャートである。

【図6】フィルタリング処理説明図である。

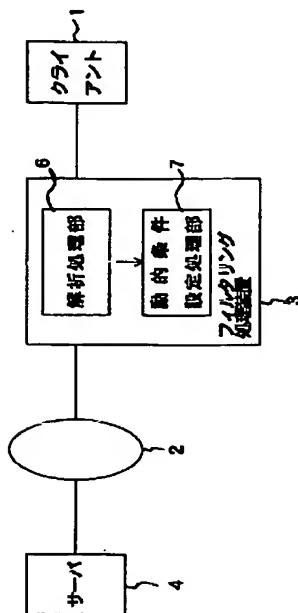
【図7】従来技術説明図である。

【符号の説明】

- 1 クライアント
- 2 インターネット
- 3 ファイアウォール
- 4 サーバ
- 5 中継処理部
- 6 解析処理部
- 7 動的条件設定処理部
- 8 アドレスポートテーブル
- 9 中継モジュール
- 10 フィルタ処理部
- 11 動的条件テーブル
- 12 静的条件テーブル

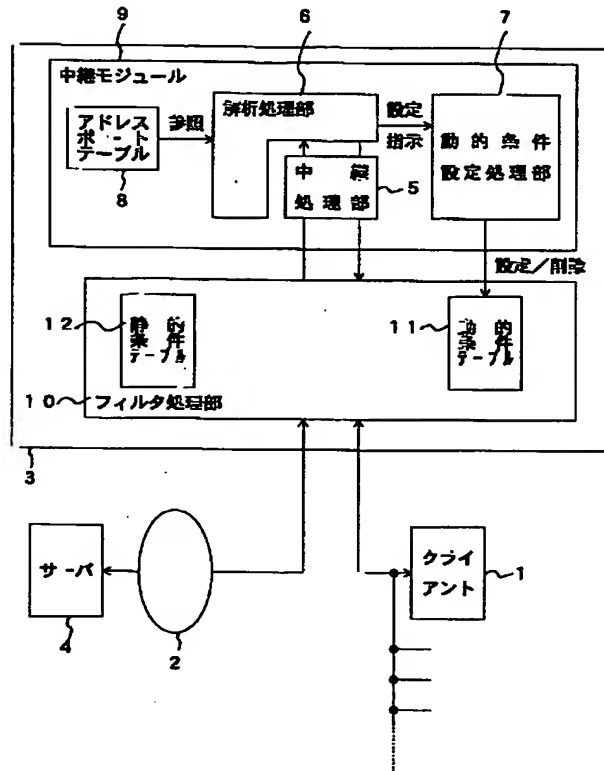
【図1】

本発明の原理構成図

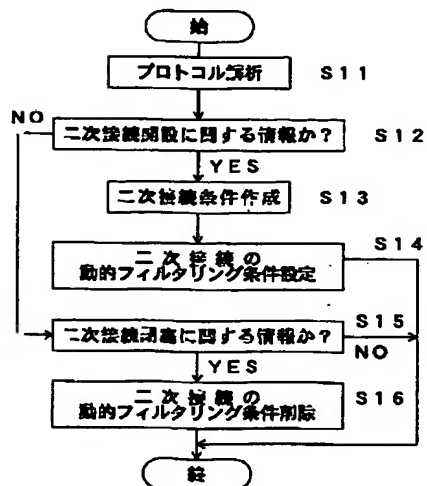


【図2】

フィルタリング処理装置説明図

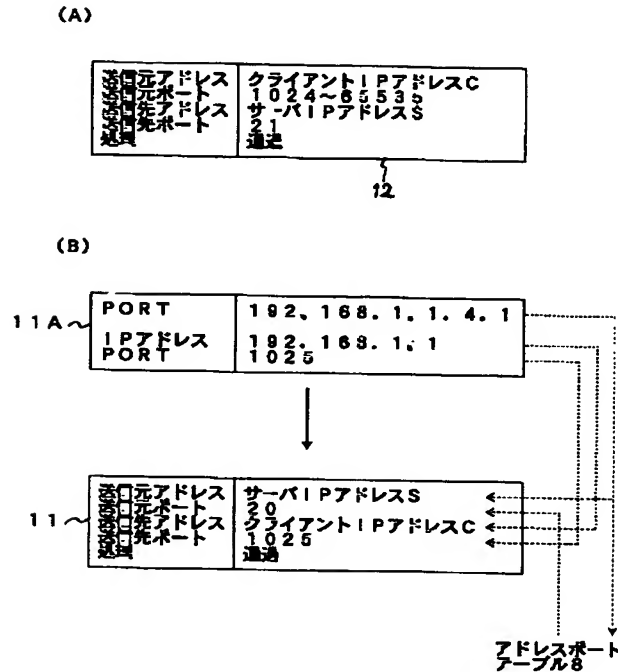


【図5】

フィルタリング条件設定処理
フローチャート

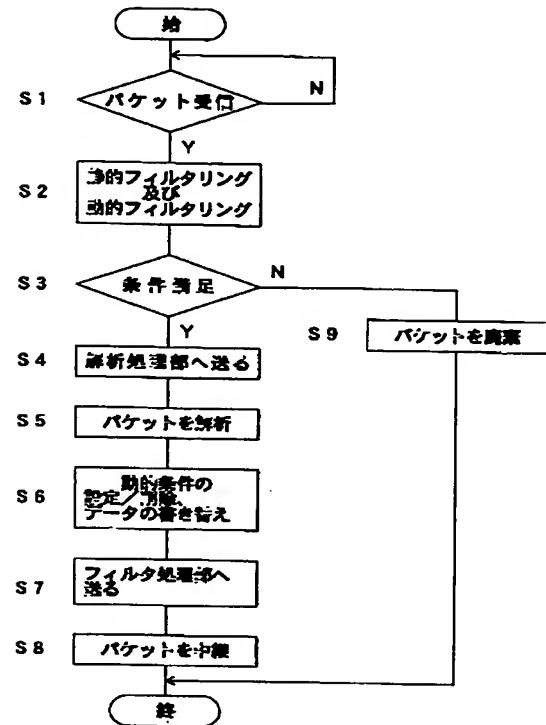
【図3】

フィルタリング条件説明図



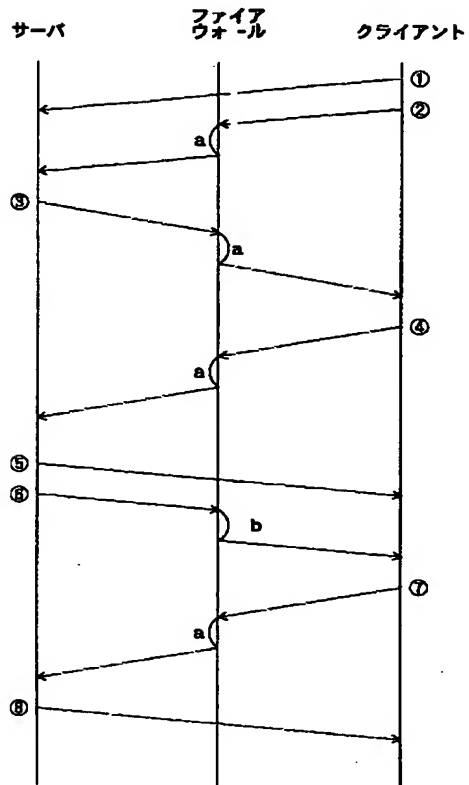
【図4】

フィルタリング処理フローチャート



【図6】

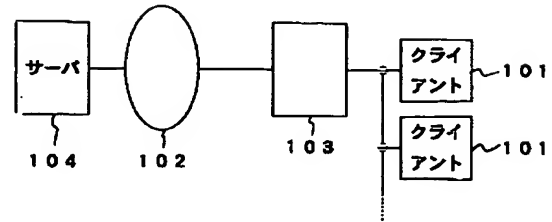
フィルタリング処理説明図



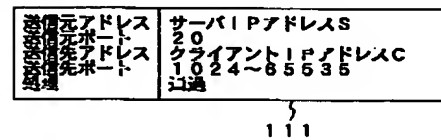
【図7】

従来技術説明図

(A)



(B)



フロントページの続き

Fターム(参考) 5B089 GA11 GA21 HA10 HB04 JA40
 KA17 KB13 KC52 KC58
 5K030 GA15 HC01 HC14 HD03 HD06
 KA07 LA01 LC15 LD20 LE17
 MA04 MB00
 5K033 AA01 AA03 CB03 CB06 CB08
 DA05 DB12 DB14 DB16 DB18
 DB20

THIS PAGE BLANK (USPTO)

Reference 3

JP 2000-32052 A

[0045] (A) In a case where a bandwidth reservation request arrives from a bandwidth reservation protocol of another router under such a condition that all bandwidths of routes between routers are used for transmitting packets, the router negotiates with an adjacent router, if the adjacent router is one according to this invention, to request use of one of sub-routes between them for the bandwidth reservation. If the adjacent router is a conventional one, the router performs a process according to a general RSVP.

[0046] (B) If a sub-route for the bandwidth reservation is set between the routers as a result of the negotiation, the router changes a routing table. In a general case of RSVP, the routing table contains destination IP address (network address), source IP address, destination port number, source port number, IP address of next router, and interface for next router (packet transfer means in this specification).

[0047] In this embodiment, as sub-route to a next router, there are plural routes, not one route. Therefore, the routing table specifies a plurality of output side packet transfer means. At the time of bandwidth reservation, the routing table is changed so as to specify an output side packet transfer means connected to a corresponding sub-route for a packet flow (one of entries of routing table) that needs bandwidth reservation.

[0048] (C) In a case where the bandwidth reservation can be made as a result of the negotiation (in a case where a sub-route for bandwidth reservation cannot be set between the routers), the transmission side transmits the packet by using an output-side packet transfer means for the sub-route set for the bandwidth reservation, and the receiving side receives the signal by using an input-side packet transfer means corresponding to the reserved sub-route.

(D) The reserved bandwidth becomes free because of a bandwidth release process by the bandwidth reservation protocol or time-out, and then all bandwidths between the routers can be used as usual.

[0049]

Next, an example of an operation flow in a case of using a method for unexplicitly performing bandwidth reservation will be described. In general, a bandwidth reservation protocol informs the router of a bandwidth reservation request, an above-described operation to keep a sub-route is performed for the bandwidth reservation in response to the request. By applying the same operation to high-priority packets, high throughput can be realized in an entire network.

THIS PAGE BLANK (USPTO)